REMARKS

Claims 1-43 are pending in this application. In the Office Action, the Examiner rejected Claims 1-7, 11-16, 17, 22, 25-32, 35-37 and 41-43 under 35 U.S.C. §102 as being fully anticipated by European Patent Application No. 0 715 242 A1 (Takashima). Also, the Examiner objected to Claims 8-10, 23, 24, 33, 34 and 38-40 as being dependent upon rejected independent claims, and indicated that these claims would be allowed if appropriately rewritten.

Claims 8, 23, 33, 38 and 39 are herein being rewritten in independent form. In particular, Claim 8 is being rewritten in independent form including the limitations of Claims 1 and 2, and Claim 23 is being rewritten in independent form including the limitations of Claim 14. Claim 33 is being rewritten in independent form including the limitations of Claims 28, 30 and 32; Claim 38 is being rewritten in independent form including the limitations of Claims 35, 36 and 37; and Claim 39 is being rewritten in independent form including the limitations of Claim 35.

It is believed that these amendments place Claims 8, 23, 33, 38 and 39 in condition for allowance without further argument. In addition, Claims 9 and 10 are dependent from Claim 8 and are allowable therewith; and Claim 24 is dependent from, and is allowable with, Claim 23. Similarly, Claims 34 and 40 are dependent from and are allowable with Claims 33 and 39 respectively.

The Examiner is, accordingly, respectfully asked to reconsider and to withdraw the objections to Claims 8-10, 23, 24, 33, 34 and 38-40, and to allow these claims.

In addition, independent Claims 1, 14, 28, 35 and 41 are being amended to better define the subject matters of these claims. For the reasons advanced below, Claims 1-7, 11-16, 17-20,

25-32, 35-37 and 41-43 patentably distinguish over the prior art and are allowable. The Examiner is thus asked to reconsider and to withdraw the rejection of these Claims under 35 U.S.C. §102, and to allow these claims.

As discussed in detail in the present application, this invention, generally, relates to methods and systems for securely handling an information unit by a first processing device interacting with a second processing device. More specifically, in accordance with the invention, information, in an encrypted form, is provided from an issuer to the first information device, such as a card reading terminal. A key needed to decrypt that information is on a second device, such as a card. Use of the second device at the first device allows the latter device to decrypt the information.

Takashima discloses a procedure for downloading digital information in a protected manner. In this procedure, encrypted information is sent to a terminal device, and a computer card is used in the decryption of that information.

While there are similarities between the present invention and the procedure shown in Takashima, there also are important differences.

The goal of Takashima's procedure is to ensure that data downloaded from a server to a device can only be used on that device. Takashima is addressing, for example, the scenario where a user downloads trial software and then calls to the software company to buy the full license, and the software company gives the user the key to enable the full functionality of the software. That key, however, could also be used on a second computer to enable the software. This is what Takashima wants to prevent.

PAGE 23/28 * RCVD AT 4/15/2004 3:56:31 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:5167424366 * DURATION (mm-ss):08-36

A general goal of the present invention is also to download data/software to a device. A more specific objective of this invention, though, is to ensure that the data downloaded was not altered and therefore that only the correct data gets onto the device. Especially in a distributed system with terminals and smart cards, this invention solves, for example, the problem of downloading a new function to a terminal to upgrade that terminal to work with smart cards from a particular issuer in a way that can be trusted. The card issuer wants to ensure that only the correct code works with his smart cards. In Takashima's scenario, the device is owned by the user. With the procedure of this invention, the device may be owned by the card issuer and they want to control what happens with the card.

Referring to Takashima, column 2, this reference describes the following steps:

a) authentication between the devices,

b) user authentication,

c) requesting data,

d) sending work key from server to device,

e) sending another work key back from the device to the server,

f) receiving random number from the server, process and forward it to the device,

g) encrypt information using the work key,

h) received data, process it and forward it to the device,

i) send a receipt back to the server.

The Examiner especially refers to Columns 2, lines 32-50, which describe steps (f) – (i).

As can be seen by looking at Figure 2a of the present application, the above steps of Takashima are very different from the preferred embodiment of this invention.

PAGE 24/28 * RCVD AT 4/15/2004 3:56:31 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:5167424366 * DURATION (mm-ss):08-36

With this preferred embodiment, a typical download that ensures that only certified components are loaded in the device which is accessed by the chip card can be done in the following way:

1. The software in the computer or a terminal requests a card with specified characteristics.
2. The smart card is inserted in the reader.
3. The software in the host computer determines that there is no support for this service for the inserted chip card available on this computer.
4. The missing service is now downloaded including the attached command to decrypt the key "T" by the chip card using the issuer's certificate and key "Ti" stored on the chip card.
5. The command is sent to the chip card and the chip card decrypts the key "T."
6. The key "T" is given back to the trusted software in the computer and it tries to decrypt the service with the given key.
7. External authentication with key "C" is used to verify that the version of the software module matches the smart card.

As can be seen, a few key differences between Takashima and the preferred embodiment of the present invention are:

PAGE 25/28 * RCVD AT 4/15/2004 3:56:31 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:5167424366 * DURATION (mm-ss):08-36

1. The flow of the encrypted data is different. Takashima sends the work key back and forth. The preferred embodiment of the present invention is much more streamlined, as the download preferably contains a command (APDUA), which includes the key to decrypt the data. That command is then sent to the card to decrypt the key used to encrypt the downloaded data.
2. With the preferred embodiment of this invention, data is directly downloaded to the device.

Basically, thus, the only common features of the Takashima procedure and this invention are that in both data is downloaded and keys are used to secure the data. However, the specific procedures are completely different.

Independent Claims 1, 14, 28, 35 and 41 are being amended to better distinguish the functions and roles of the first and second information processing devices. In particular, Claims 1 and 41 are being amended to indicate that the information unit is transmitted from the issuer to the first processing device, in an encrypted form. Claim 14, which is directed to a system for securely handling an information unit, is being amended in include analogous apparatus limitations.

Claim 28 is directed to a chip card for securely handling an information unit by interoperating with an information handling terminal device. This claim, as presented herewith, includes means for transmitting at least one key to that handling device, to enable that device to decrypt an information unit that was received that device, in encrypted form, from an issuer.

PAGE 26/28 * RCVD AT 4/15/2004 3:56:31 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:5167424366 * DURATION (mm-ss):08-36

Claim 35 is directed to a chip card accepting device, and describes means for receiving at least one key from a chip card, and means for using that key to decrypt an information unit, which was received by the accepting device in an encrypted form.

With these changes to the claims, it is believe clear that the computer card 3 shown in Takashima cannot be considered to be the first information processing device, as described in Claims 1, 14 and 41, the terminal device described in Claim 28, or the card accepting device described in Claim 35.

The other references of record have been reviewed, and it is believed that these other references, whether considered individually or in combination, are no more pertinent than Takashima. For instance, WO 98/03904, which was cited for the first time in the last Office Action, discloses a procedure for downloading encrypted data from a server. This procedure uses standard public/private key technology and a smart card, as described in the Background Section of the present application as prior art.

Because of the above-discussed differences between Claims 1, 14, 28, 35 and 41 and the prior art, and because of the advantages associated with those differences, these Claims 1, 14, 28, 35 and 41 patentably distinguish over the prior art and are allowable. Claims 2-7 and 11-13 are dependent from Claim 1 and are allowable therewith; and Claims 15-22 and 25-27 are dependent from, and are allowable with, Claim 14. Also, Claims 29-31 are dependent from Claim 28 and are allowable therewith; Claims 36 and 37 are dependent from, and are allowable with, Claim 35; and Claims 42 and 43 are dependent from Claim 41 and are allowable therewith. The Examiner is, hence, respectfully requested to reconsider and to withdraw the rejections of Claims 1-7, 11-16, 17-20, 25-32, 35-37 and 41-43 under 35 U.S.C. §102, and to allow these claims.

PAGE 27/28 * RCVD AT 4/15/2004 3:56:31 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:5167424366 * DURATION (mm-ss):08-36

Every effort has been made to place this application in condition for allowance, a notice of which is requested. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is asked to telephone the undersigned.

Respectfully submitted,

John S. Sensny

John S. Sensny
Registration No. 28,757
Attorney for Applicants

SCULLY, SCOTT, MURPHY & PRESSER
400 Garden City Plaza
Garden City, New York 11530
(516) 742-4343

JSS:jy

PAGE 28/28 * RCVD AT 4/15/2004 3:56:31 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:5167424366 * DURATION (mm-ss):08-36